THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF: 8172 ARTILLERY CIRCLE, BUILDING 1273, FORT LEONARD WOOD, MISSOURI, INCLUDING ANY AND ALL LOCKERS AND STORAGE AREAS UTILIZED BY STAFF SERGEANT ERIK FINSTER

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Jeffrey H. Burnett, a Task Force Officer (TFO) with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state as follows:

1. I have been employed as a police officer with the City of Springfield, Missouri, since May 1999. I am currently a TFO with the FBI, as well as a member of the Southwest Missouri Cyber Crimes Task Force. I have been assigned to investigate computer crimes to include violations against children. I have gained expertise in the conduct of such investigations through training in seminars, classes, and every day work related to conducting these types of investigations. I have attended training provided by the FBI Cyber Crime Division, the FBI's Regional Computer Forensic Laboratory, National White Collar Crime Center (NW3C), and the Missouri Internet Crimes Against Children (ICAC) Task Force. I have written, executed, and assisted in over 300 search warrants on the state and federal level.

2. As a TFO, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. The

statements in this affidavit are based on my personal observations, my training and experience, my investigation of this matter, and information obtained from other agents and witnesses. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth the facts that I believe necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2251, 2252, and 2252A are currently located at **8172 Artillery Circle, Building 1273, Fort Leonard Wood, Missouri, including any and all lockers and storage areas utilized by Staff Sergeant Erik Finster**, which is located in the Western District of Missouri.

3. I make this affidavit in support of an application for a search warrant for evidence, fruits, and instrumentalities of the forgoing criminal violations, which relate to the knowing possession, receipt and production of child pornography. The property to be searched is described in the following paragraphs and in Attachment A. I request authority to search and/or examine the seized items, specified in Attachment B, as instrumentalities, fruits, and evidence of crime.

4. I have probable cause to believe that evidence of violations of 18 U.S.C. §§ 2251, 2252, and 2252A, involving the use of a computer in or affecting interstate commerce to receive, possess and produce child pornography, is located in and within the aforementioned property described below. Thus, as outlined below, and based on my training and experience, there is probable cause to believe that

evidence, fruits, and/or instrumentalities of the aforementioned crimes are located in this property.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of Title 18, United States Code, Sections 2251, 2252, and 2252A, relating to material involving the sexual exploitation of minors:

a. 18 U.S.C. § 2251(a) prohibits a person from employing, using, persuading, inducing, enticing, or coercing a minor to engage in sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce, or if such visual depiction actually was transported in or affecting interstate commerce.

b. 18 U.S.C. § 2252 prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such visual depiction was produced using materials that had traveled in interstate or foreign commerce.

c. 18 U.S.C. § 2252A prohibits a person from knowingly mailing, transporting, shipping, receiving, distributing, reproducing for distribution,

or possessing any child pornography, as defined in 18 U.S.C. §2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce.

DEFINITIONS

6. The following definitions apply to this Affidavit and its Attachments:

a. The term "minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

b. The term "sexually explicit conduct," 18 U.S.C. § 2256(2)(A)(i-v), is defined as actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.

c. The term "visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

d. The term "computer," as defined in 18 U.S.C. §1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data

processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

e. The term "child pornography," as defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

f. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic, or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks,

CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).

g. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

h. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

i. "Domain names" are common, easy to remember names associated with an IP address. For example, a domain name of "www.usdoj.gov" refers to the IP address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period.

j. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

7. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed.

8. Computers basically serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking.

9. With digital cameras, images of child pornography can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

10. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

11. The Internet affords individuals several different venues for meeting one another,

obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

12. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

13. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer

files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space -- that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space -- for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

CELLULAR PHONES AND CHILD PORNOGRAPHY

14. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law

enforcement officers with whom I have had discussions, cellular phones have likewise revolutionized the manner in which child pornography is produced and distributed.

15. Cellular phones ("cell phones") are exceptionally widespread. The Central Intelligence Agency estimates that in 2016 there were 416 million cell phone subscribers in the United States. Cell phones increasingly offer features such as integrated digital cameras, the ability to store hundreds of digital images and the ability to access and browse the Internet.

16. In my training and experience, the ready availability and personal nature of cell phones has led to their frequent use in the commission of child pornography offenses. Individuals with a sexual interest in children will often use their cell phone to browse the Internet and to distribute, receive, and store child pornography files. Individuals producing child pornography will also frequently use the integrated digital camera within a cell phone to produce the images, and then store the images both on the phone and on other devices – such as computers and computer storage media.

17. Cell phones, like other computer systems, will frequently retain data relating to activities, such as Internet browsing history, digital images, and other digital data, that can remain stored for a long period of time.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS AND CELL PHONES

18. Searches and seizures of evidence from computers and cell phones commonly

require agents to download or copy information from the devices and their components, or seize most or all computer items (computer hardware, computer software, and computer-related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish fully on-site.

b. Searching computer systems and cell phones for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-

protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

19. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit ("CPU"). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

20. Furthermore, because there is probable cause to believe that the computer, its storage devices, and cell phones are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

BACKGROUND OF THE INVESTIGATION

21. On June 13, 2019, the National Center for Missing and Exploited Children (NCMEC) generated a Cybertipline Report (CTR) after receiving information from Yahoo! Inc., indicating that a user with a screen name "erik erik" and the username "XBXWLWSBSEPBCD3ACWLVCRATWY," uploaded eight images of suspected child pornography to its servers on May 5, 2019. Further information

provided in the CTR indicated that the username was linked to the following e-mail addresses: erikqwerty@yahoo.com, efinster@yahoo.com, and erikfinster@yahoo.com. The user also had two other Yahoo!, Inc., screen names identified as "erikqwerty" and "erik.finster."

22. Detective T. Hicks of the Springfield, Missouri, Police Department was assigned the investigation. After reviewing the information contained in the CTR, Detective Hicks determined that there was an individual named ERIK FINSTER, residing at 3315 West Chestnut Expressway, Springfield, Missouri, and who was enlisted in the Missouri National Guard. Additionally, Detective Hicks discovered that FINSTER was married and the father to at least three minor children.

23. Detective Hicks reviewed the eight images submitted with the CTR that were uploaded by the aforementioned user to servers operated by Yahoo!, Inc. Detective Hicks concluded that four of the images contained depictions of child pornography and the other images were deemed to be child erotica.

24. On June 26, 2019, Detective Hicks served a search warrant issued under color of Missouri law to Yahoo! Inc., to obtain information contained in the three e-mail accounts referenced above. On July 2, 2019, Detective Hicks received data from Yahoo!, Inc. in response to the search warrant.

25. During the review of the content of the data, Detective Hicks located photographs of the user. The photographs in the data were compared to photographs of FINSTER obtained from the Missouri Department of Revenue. Detective Hicks was able to confirm that the "Erik Finster" residing at 3315 West Chestnut

Expressway, Springfield, Missouri, was the same individual using the Yahoo! e-mail addresses in question.

26. During the review of data contained in account "erikqwerty@yahoo.com," Detective Hicks observed several e-mails of investigative interest. Specifically, the data indicated that FINSTER had exchanged messages with individuals on Craigslist and Doublelist, discussing sexual interest in children.

27. In one such exchange with a user identified as "im4fun334@yahoo.com," FINSTER received images of minor females in bathing suits from the other user, that were identified as his step-daughter and friends. FINSTER then responded by transmitted a message stating, "I've came on my young daughter's panties. It was such a thrill." FINSTER sent the other user a series of photographs of a minor child identified as Jane Doe #1[1]. Several photographs depicted Jane Doe #1 attired in her underwear and bra. Some images focused on Jane Doe #1's underwear. After receiving the images, the user identified as "im4fun334@yahoo.com" replied, "Oh my! I think I'll cum on her if that's ok….. I wouldn't touch her of course but in OUR world…..delicious!" FINSTER replied "Sure. I like that. Want to cum on her face? Or I can crop more pics." The user then told FINSTER he should give her Benedryl and ejaculate on her stomach. FINSTER indicted he liked that idea and sent additional photos of Jane Doe #1. The two continued to have more sexual conversations about children then FINSTER stated "I'd be happy to get you off to my dau."

1 Jane Doe has been identified by Detective Hicks.

28. Det. Hicks reviewed another conversation between FINSTER and a Craigslist user identified as "j5xxm-6437412795@pers.craiglist.org." During the chat exchange, which began in early January 2018, the user transmitted to FINSTER six videos that depicted child pornography. FINSTER indicated that he enjoyed the videos.

29. On July 3, 2019, I, along with Detective Hicks and other law enforcement personnel served a search warrant, issued by the Circuit Court for Greene County, Missouri, on FINSTER's residence, located at 3315 West Chestnut Expressway, Springfield, Missouri.

30. FINSTER was located within the residence and questioned. After waiving his *Miranda* rights, FINSTER acknowledged he was the sole user of Yahoo! account "erikqwerty@yahoo.com." FINSTER further confirmed that he had participated in the above-described conversations, during which he received videos depicting child pornography. FINSTER admitted to sending images of children to other individuals via the Internet, but claimed that he did not think that they were illegal because he found them utilizing a Google search. FINSTER also acknowledged to sending images of Jane Doe #1 and Jane Doe #2[2], via the Internet, to other individuals for use during masturbation. During the interview, FINSTER informed the investigators that he had three computers at his office located at 8172 Artillery Circle, Building 1273, Fort Leonard Wood, Missouri, one personal laptop and two governmental computers. FINSTER advised that he had activated a new

2 Jane Doe #2 has been positively identified by Detective Hicks as an adult female.

phone approximately one month ago, because he claimed his old phone quit working and was disposed of.

31. FINSTER's spouse was interviewed on scene. Ms. Finster told the investigators that she had no knowledge of FINSTER's online activities. Ms. Finster indicated that she was unable to locate his old phone at her residence and further informed the investigators that FINSTER does not typically dispose of such things.

32. On July 9, 2019, I contacted United States Army, Criminal Investigation Division (CID) Investigator Sean Diemler. Investigator Diemler contacted FINSTER's superior officer, Chief Warrant Officer (CWO) Andrea Lawrence, and inspected FINSTER's work area/temporary quarters located at 8172 Artillery Circle, Building 1273, Fort Leonard Wood, Missouri. Inside FINSTER's work area, Investigator Diemler located two laptops in plain view. FINSTER's personal computer was identified as a Toshiba Satellite Laptop, serial number 2C205480Q. FINSTER's government owned computer was identified as a Dell Latitude laptop, serial number 1NRJPL2. Investigator Diemler and CWO Lawrence placed the laptops in a secured container to ensure no one would tamper with the items.

33. Investigator Diemler relayed that FINSTER had a personal storage locker located in the same facility that likely contained FINSTER's personal property. The locker was secured with padlocks attached by FINSTER. The locker had a placard that displayed "RTS-M, 5th ORD BN SSG FINSTER, Locker #90." Investigator Diemler also observed several CD/DVD's in a locker behind FINSTER's desk area.

PROBABLE CAUSE

34. Based on the above facts, I believe probable cause exists for the issuance of a warrant to search the premises described more fully in Attachment A for (1) property that constitutes evidence of the commission of a criminal offense; (2) contraband, the fruits of a crime, or things otherwise criminally possessed; and/or (3) property designated or intended for use or which is or has been used as the means of committing a criminal offense, namely possible violations of Title 18, United States Code, Sections 2251, 2252, and 2252A, including but not limited to the items listed in Attachment B.

Jeffrey Burnett
Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn before me this 25th day of July, 2019.

David P. Rush
United States Magistrate Judge
Western District of Missouri